MANAV RACHNA INTERNATIONAL UNIVERSITY

Research Plan

For

Ph. D. Programme 2009-10

Title: An Improvised Mechanism to Enhance Computer Network Security.

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

FACULTY OF ENGINEERING & TECHNOLOGY

Submitted by:
Name: Kuldeep Tomar
Signature:
Registration No: 09019990371

Supervisor:
Name: Prof. (Dr.) S. S Tyagi
Signature:
Designation: Professor
Department of Computer Science &, Engineering, FET, MRIU, Faridabad.

Co-Supervisor:
Name: Prof. (Dr.) Ranjit Biswas
Signature:
Designation: Professor
Department of Computer Science, Jamia Hamdard, New Delhi.

Abstract

In today's scenario Computer Security is the basic need of any growing organization as they have developed complex data centers and networks. Lots of data is required to be transferred and processed across network. Many Organizations are using different types of security mechanism to make their computers network secure but due to rapid change in technology they are not suffice. Thus there is a much need of development of improvised mechanism to counter security threats, breaches in a computer network.

Mechanism like Intrusion detection and prevention systems are quite effective to enforce security standards, but still have many possibilities of improvisation to provide higher standard of computer network security.

Our aim of research is to suggest a better mechanism to counter current challenges in this dynamic scenario, to do this we would study current threats, their vulnerability to our systems. Our focus also would be on studying available tools and mechanism like Intrusion detection system, Linux based security mechanism etc. Our work may consolidate major issues, merits of existing system and would be able to able to propose/ develop better mechanism/ solution which may set guidelines for better computer's/ network security.

Keywords: Security, Network, IDS, Mechanism, Threats.

TABLE OF CONTENTS

S. No	Topic	Page No
1.	Introduction	01
2.	Literature Review	05
3.	Description of Broad Area/Topic	07
4.	Objectives of the study/problem identification	10
5.	Methodology	11
6.	Proposed / expected outcome of the research	12
7.	References	13

1. Introduction

Past few decades there is vast increase in the usage of Internet, Intranet and electronic devices, resultant of which the incidents of security breaches, cyber attacks, and security threats in a computer network has increased. With this many criminal activities has arisen that takes the advantage of internet, latest technology based tools and available wired or wireless electronic resources for computer crimes like theft of Information, data manipulation and other computer frauds. There is a big challenge to keep our self updated with the latest security challenges in computer networks.

Thus there is a much need for the study of Computer network, Internet and Intranet security and available options for reducing or minimizing them. There are lots of tools are available to counter these threats, but due to rapid change in technology sometimes they are not enough. Intrusion detection systems are one of the effective technologies available these days. Therefore our area of the research work would be computer network security challenges and development of "An improvised mechanism to Enhance Security of Computer Network".

1.1 Introduction to Computer Networks

The computer network may be defined as an interconnection between two or more computers by communication paths. We say that two computers are interconnected if they are able to exchange information. This connection may be via a copper wire, fiber optics, radio waves, microwaves or communication through satellites. An autonomous computer means self-controlled computer system, having own operating system, memory and control unit.

1.2 Types of Computer Networks

Depending upon how the computer communicate between them there are various types of computer networks, based upon size of network, what topology they adopt, etc. Broadly speaking these computer networks are classified as: Local Area Networks (LAN), Metropolitan Area Networks (MAN), and Wide Area Networks (WAN). All computers in such computer networks work in similar way and the geometric arrangement of actual physical organization of computers (and other network devices) in a network is called topology.

1.2.1 Internet

Internet is a network of networks. A means of connecting a computer to any other computer anywhere in the world through dedicated routers and servers. When two computers are connected over the Internet, they can send and receive all kinds of information such as text, graphics, voice, video, and computer programs.

No one owns Internet, although several organizations the world over collaborate in its functioning and development. The high-speed, fiber-optic cables through which the bulk of the Internet data travels are owned by telephone companies in their respective countries. The Internet grew out of the Advanced Research Projects Agency's Wide Area Network (then called ARPANET) established by the US Department Of Defense in 1960s for collaboration in military research among business and government laboratories. Later universities and other US institutions connected to it. This resulted in ARPANET growing beyond everyone's expectations and acquiring the name 'Internet.' The development of hypertext based technology (called World Wide web, WWW, or just the Web) provided means of displaying text, graphics, and animations, and easy search and navigation tools that triggered Internet's explosive worldwide growth.

1.3 Intranets: Organization Centric Networks

An Intranet is a logical network that is used by the personnel of an organization to access or store sensitive, proprietary information, which individuals outside the organization cannot access or Intranet is the generic term for a collection of private computer networks within an organization. Every organization has a network for its functioning and storage of sensitive data. These computers must function smoothly in an integrated way and must have access to outside of the organization only through official channel usually through a server. Such a network is called Intranet. Thus an Intranet is a private network that is contained within an enterprise. The Intranet may consist of many interlinked local area networks and also use leased lines in the wide area network. Typically, an intranet includes connections through one or more gateway computers to the outside Internet. The main purpose of an intranet is to share company information and computing resources among employees.

Typically, in big organizations allow users within their intranet to access the public Internet through firewall servers that have the functionality to inspect messages in both directions so that company security is maintained. When a part of intranet is made accessible to suppliers,

customers, or others outside the company, that part becomes part of an extranet. In many organizations, intranets are protected from unauthorized external access by means of a network gateway, IDS and firewall.

1.4 Security Issues in Computer Networks

There are many security issues in a computer network. Latest security concerns and issues are discussed below.

- Poor configuration, deployment of appropriate security detection, prevention mechanisms and tools.
- Users form a network access such websites from which malicious programs can be injected to internal network by which secret information can be compromised or get manipulated.
- Manipulation with router updates can cause traffic to flow to unauthorized destinations. These kinds of attacks are sometimes called “route injection” attacks.
- When an attacker manipulates IP packets to falsify IP addresses then masquerading attack takes place. Masquerades can be used to inject false data into a network or gain unauthorized access.
- If an attacker can insert falsified IP packets after session establishment via IP spoofing, sequence number prediction and alteration, or other methods then Session hijacking attack may take place.
- The land attack involves sending a packet to the router with the same IP address in the source and destination address fields, and with the same port number in the source port and destination port fields. This attack may cause denial of service or degrade the performance of the router.
- TCP SYN attack and the TCP SYN Attack involve transmitting a volume of connections that cannot be completed at the destination. This attack causes the connection queues to fill up, thereby denying service to legitimate TCP users.

Organizations must deploy a comprehensive detection system to constantly map and monitor activities to prevent hackers from slipping anything past their networks’ defenses. It’s the role of network administrator to deploy an efficient mechanism for Identification, authorization and to keep track of activities being logged and looked upon.

1.5 Firewall

A Firewall is a system that keeps out unauthorized or unwanted traffic. Thus the first major improvement in network security was the firewall. It is a system that denies permits and inspects computer traffic between networks based on set of rules. There are certain limitations of firewalls few are;

- Firewalls cannot disable worms or virus or other malicious activities.
- Generally a firewall should meet the speed of connection otherwise it may pass unmonitored data.
- For some individuals or small business organizations firewalls can be costly.
- Security risks such as social engineering cannot be handled by firewalls.
- Misuse of passwords or password policies cannot be enforced by firewalls.
- Firewall sometimes cannot block pop-ups ads or junk email.
- Firewalls cannot stop internal users from accessing websites with malicious code.

1.6 Intrusion Threats to Networks

Wired and wireless networks are growing day by day, lots of important and private information is stored in the networks. Many a times networks are compromised and valuable information is taken by hackers. This is because of weak defenses in network to the intruders. There are many types of intrusion threats to networks which should be taken care by organizations to be secure, few of them are:

- Spywares, viruses & Worms.
- Steal of Information.
- Denial of Service.
- IP Spoofing.
- Brute force attacks.
- Web application vulnerability scanning etc.

There are many tools to counter security issues in computer network for example Firewall, IDS etc. IDS are one of the efficient tools to counter network security, lots of work has been done to improvise IDS efficiency, and still there are areas of improvisation.

2. Literature Review

Several intrusion detection systems have been proposed in the literature and implemented. At very early stage J. P. Anderson [1] brought out a technical report on "Computer Security Threat Monitoring and Surveillance" in April 1980 to elaborate the concept of intrusion in a Network. There after Dorothy Denning [5] presented "An Intrusion Detection Model" to identify and formulate the approaches to develop the Intrusion detection systems. Most of the IDS's are derived from this statistical intrusion detection model of Dorothy Denning. Some IDSs use the audit trail generated by the computer or try to analyze intrusions by analyzing network connections and the flow of information in a network. Others still, such as DIDS [27] have expanded the scope of detection by distributing anomaly detection across a heterogeneous network and centrally analyzing partial results of these distributed sources to detect potential intrusions that may be missed by the individual analysis of each source.

N. Puketza, K. Zhang, M. Chung, B. Mukherjee, and R. A. Olsson [16] presented a methodology for testing intrusion detection systems. They carried out details of the methodology, including strategies for test-case selection and specific testing procedures. These tests-formulation techniques are taken from the field of software testing. They included quantitative results from testing experiments on the Network Security Monitor (NSM). They also presented an overview of the software platform consisting of the UNIX tools to create user-simulation scripts for testing experiments.

Jim Yuill, S. Felix Wu, Fengmin Gong, Ming-Yuh Huang, [31] considered Intrusion Detection for an On-Going Attack on the system. They assumed that prior to an attack the IDS operates in anticipation of a general threat, whereas during an attack it can deal more about attackers and attacked devices. Thus a profile of the attacker is developed and then using this information, the system reveals about himself during his attacks. They tried to predict the attacker's behavior based on estimates of his asset-appraisal, attack-costs and attack-resources.

Peter Mell and Mark McLarnon [19] developed "Mobile Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems". In their approach, they assumed that an attacker can disable a system by taking out a node high in the hierarchy, thus amputating a portion of the distributed system. Further, they provided a solution to this problem; that is to cast the internal nodes in the system hierarchy as mobile agents. These mobile agents randomly move around the

network such that an attacker is unable to locate their position. If an attacker takes out a mobile agent platform, the remaining agents estimate the location of the attacker and automatically avoid those networks. Killed agents are resurrected by a group of backups that retain all or partial state information.

H. Debar and A. Wespi [9] adopted a new approach comprising of Aggregation and Correlation of Intrusion-Detection Alerts to develop IDS. They describe an aggregation and correlation algorithm used in the design and implementation of an intrusion-detection console built on top of the Tivoli Enterprise Console (TEC). The aggregation and correlation algorithm aims at acquiring intrusion-detection alerts and relating them together to expose a more condensed view of the security issues raised by intrusion-detection systems.

Robert F. Erbacher, Kenneth L.Walker, and Deborah A. Frincke [7] have worked on Intrusion and Misuse Detection in Large-Scale Systems. The major effort was to identify an attack before an organization incurs damage, loses information (theft or otherwise), or has its integrity impugned. They presented information visualization techniques based on a glyph metaphor for visually representing textual log information.

Emilie Lundin Barse [6] presented a Logging for intrusion and fraud detection system based on the log data problems in intrusion and fraud detection. This technique included a methodology for determining exactly which log data that can be used for detecting specific attacks. In the ideal situation they could collect exactly the data needed for detection and develop more efficient and adapted log sources.

Stefan Axelsson [29] made efforts for Understanding Intrusion Detection through Visualization and analyzed as to why false alarms, which are produced in high number in our systems, are and will remain a problem. He proposed to apply results from the field of information visualization to the problem of intrusion detection. The visualization helped the operator either detect the attacks it and more importantly the false alarms.

Tao Peng, Wanli Zuo [18] developed a data mining-based network intrusion detection framework in real time (NIDS). The proposed system is implemented as a distributed architecture consisting of sensor, data preprocessor, extractors of features and detectors. To improve efficiency, they adopted a novel FP-tree structure and FP-growth mining method to extract features based on FP-tree without candidate generation.

V. Venkatachalam, S. Selvan [30] developed Intrusion Detection System using Improved Competitive Learning technique of Neural Network. Their further investigation included the time taken for training and testing, generate Confusion matrix with KDD CUP 99 data using simulation tool and compare it with five classification techniques (Gaussian Mixture, Radial Basis Function, Binary Tree Classifier, SOM, and ART). They showed that their results indicate that LAMSTAR exhibit high accuracy at the cost of long training time.

M. Rehak, M. Pechoucek and P. Celeda [14] provided an agent-based intrusion detection system designed for deployment on high-speed backbone networks. This system provides the integration of several anomaly detection techniques by means of collective trust modeling within a group of collaborative detection agents.

M. Guennoun, A. Lbekkouri and K. E. Khatib, [13] Optimized the Feature Set of Wireless Intrusion Detection Systems to detect service attacks on Wireless networks, intrusions classifiers which are built to distinguish between normal and anomalous traffic.

3. Description of Broad Area/Topic

In a network system, an intruder is defined as a program or person who attempt to and may become successful to enter into an information system or perform an action not allowed [26]. We refer intrusion as any set of activities that attempts to compromise the availability, confidentiality, or integrity of a computer resource [10]. The act of detecting actions that attempt to compromise the integrity, confidentiality, or availability of a computer resource can be referred as intrusion detection [25]. Our broad area of the research work would be computer network security and proposing/development of an improvised mechanism using IDS to Enhance Security of Computer Network.

3.1 Intrusion Detection Systems

An intrusion detection system is a device or software application that monitors network and or system activities for malicious activities or policy violations and produces reports [25].

Definition of IDS

Intrusion detection system is a security system that analyzes network traffic and computers systems for possible attacks originating from inside the organization or attacks originating from outside the organization.

3.2.1 Role of IDS

An Intrusion Detection System is one of the most effective systems to counter security breaches and listens to all the traffic that passes through a network segment. Thus IDS is first and foremost a network sniffer or if you prefer a network protocol analyzer and then looks at the traffic content to determine whether it is normal traffic or a possible attack. If the traffic is suspicious, then IDS generates alert so that further actions could be taken (Crothers, 2003).

3.2.2 Effectiveness of intrusion-detection systems

To evaluate the effectiveness of an intrusion-detection system, Porras and Valdes [20] have proposed the following three parameters:

- **Accuracy:** Accuracy deals with the proper detection of attacks and the absence of false alarms. Inaccuracy occurs when an intrusion-detection system ages a legitimate action in the environment as anomalous or intrusive.

- **Performance:** The performance of an intrusion-detection system is the rate at which audit events are processed. If the performance of the intrusion-detection system is poor, then real-time detection is not possible.

- **Completeness:** Completeness is the property of an intrusion-detection system to detect all attacks. Incompleteness occurs when the intrusion-detection system fails to detect an attack. This measure is much more difficult to evaluate than the others because it is impossible to have a global knowledge about attacks or abuses of privileges.

3.2.3 Problems with Existing Systems

There are lots of unsolved problems, challenges and issues with existing systems and few needs more improvisation few of the issues are [15] are addressed below.

- Probability of false alarms.

- Probability of detection.

- Ability to correlate events.
- Ability to handle unknown attacks.

Few more challenges/ issues are:

- Problem of reliability.
- IDS are prone to DOS attacks.
- Limited Scalability etc.

3.3 Types of Intrusion Detection Systems

Intrusions Detection broadly can be classified into two main categories both have their own advantages and disadvantages. They are as follow:

Host Based Intrusion Detection: HIDSs evaluate information found on a single or multiple host systems, including contents of operating systems, system and application files.

Network Based Intrusion Detection: NIDSs evaluate information captured from network communications, analyzing the stream of packets which travel across the network.

Taxonomy of IDS

Figure below shoes the classification [23] of IDS.

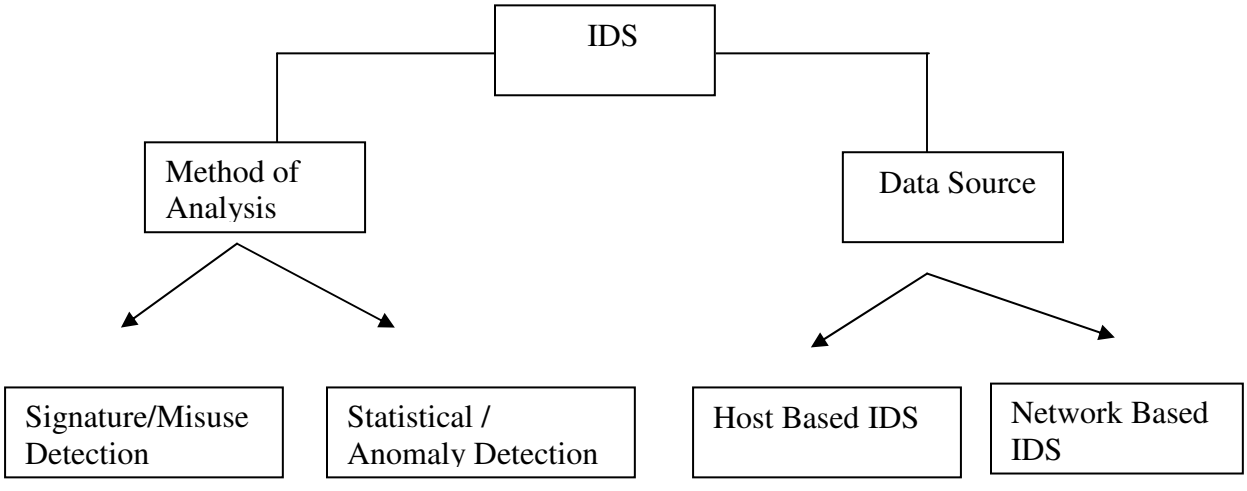

Figure (1) Taxonomy of IDS

3.4 Host Based IDS

IDSs that monitor a single system using logs or add-on software are still popular and are more precisely referred to as Host-Based Intrusion Detection Systems (HIDS). Modern HIDS typically add software loaded on the protected system that monitors for attacks. Tripwire is a classic example of HIDS software.

Many organizations have network of computer systems, all working inter-dependently. For the security of such networks, we have network-based IDSs. These Network-Based Intrusion Detection Systems are more comprehensive and have wider applications.

3.5 Network Based IDS

Network-based Intrusion Detection System (NIDS) have to be developed for the security of the network. This NIDS analysis the incoming and outgoing traffic to examine if some unauthorized access is being made or some sensitive information is being sent out. Primarily, a NIDS system listens to all the traffic on a given network segment. In doing so it is able to see both legitimate and attack traffic as it passes. Legitimate traffic is ignored while traffic that appears to be an attack will cause an alert. The nature of the alert will vary between attacks and between different NIDS software.

4. Objective of the study/problem identification

The objective of research is to suggest a better mechanism to improvise security in computer networks, to do this we would study current threats, their vulnerability to our systems. Our focus also would be on studying available tools, mechanism. Intrusion detection and prevention systems are one of the better mechanisms to counter computer network security. There are lots of research challenges/issues to get addressed few them are mentioned below:

- Identify the parameters of improvisation for making computer network less vulnerable.
- Identifying the levels or stages of security policy as if screening is done at one single point and if it is compromised then would lead to single point of failure. Also introducing more levels and stages would lead to more detection time. So an optimal solution is required.

- Identifying ways to improvise performance of IDS as in particular situation IDS may lose some packets or let's to pass under heavy traffic load.
- Other major challenges are the ability to identify unauthorized users, restricting access of internal users to access malicious sites etc.

Our work can consolidate major issues, merits, demerits of an existing system. Our work would provide better awareness among users about current threats, challenges and may set guidelines to develop better security mechanism addressing one or more above/current challenges.

5. Methodology

The methodology of the research work would be carried out in phases to obtain the main objectives of the research, to study the issues and categories of threats to our computer networks with an aim of improvising the security aspect of our computer networks by identifying major vulnerabilities and proposing or developing a mechanism for better security.

Phase 1: Study for the literature survey on the topic and work on course work subjects.

Phase 2: Working for course work exams.

Phase 3: Study available tool, mechanism and categorizing the issues and challenges with them. Comparing and evaluating disadvantages and advantages of the existing mechanism. Identify the areas of improvisation to make the computer network less vulnerable, also working for research paper publications.

Phase 4: Identifying optimal ways, parameters for minimizing security breaches and to propose or develop an improvised mechanism in a simulated environment to make more secure computer network along with research paper Publications.

Phase 5: Final report writing, reviewing of thesis and submission.

6. Proposed/expected outcome of the research

The research work carried out would provide insight knowledge of the current security threats and better counter mechanisms for them. People belonging to different disciplines would get acquaintance to these threats and it would provide a better way for preventing their resources in a computer network from security breaches. Since we know it is costly to keep updated with all the number of existing security threats and we know that no System/Mechanism can solve all security problems; but still it enforces higher standards of security. So the main aim behind this research is to update user about current issues and to develop/propose an efficient security mechanism considering the dynamic nature of today's computer network environment, as there is always a trade-off between accuracy and acceptability.

7. References

1. Anderson J. P, “Computer Security Threat Monitoring and Surveillance”, Technical report, April 1980.
2. Ashish Kamra, “Mechanisms for Database Intrusion Detection and Response”, Proceedings of the Second SIGMOD PhD Workshop on Innovative Database Research (IDAR), June 13, 2008.
3. D. Zamboni, “Using Internal Sensors for Computer Intrusion Detection”. Center for Education and Research in Information Assurance and Security, Purdue University. August 2001.
4. Dmitry S. Kazachkin, Dennis Y. Gamayunov, “Network traffic analysis optimization for signature-based intrusion detection systems”, Computational systems lab at CMC MSU. 2008
5. E. Denning Dorothy,” An Intrusion - Detection Model. In IEEE Transactions on Software Engineering”, February 1987.
6. Emilie Lundin Barse,” Logging for intrusion and fraud detection. PhD thesis”, Goteborg, Sweden, 2004.
7. F. Erbacher Robert, L Kenneth. Walker, and A Deborah. Frincke, “Intrusion and Misuse Detection in Large-Scale Systems”, January 2002.
8. Godfrey C. Onwubolu, Alok Sharma, “Intrusion Detection System using Hybrid Differential Evolution and Group Method of Data Handling Approach”. ICIM Sept, 2008.
9. H. Debar and A. Wespi. “Aggregation and Correlation of Intrusion-Detection Alerts”. Proceedings of the fourth International Symposium on Recent Advances in Intrusion Detection (RAID), October 2001.
10. K. Ilgun, R. Kemmerer, P. A. Porras, “State Transition Analysis: A Rule-Based Intrusion Detection Approch”, IEEE Transaction on Software Engineering, 1995.
11. K. Scarfone, P. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center (National Institute of Standards and Technology). February 2007.

12. M. Bahrololum and M. Khaleghi, “Anomaly Intrusion Detection System Using Hierarchical Gaussian Mixture Model”. IJCSNS International Journal of 264 Computer Science and Network Security, August 2008.
13. M. Guennoun, A. Lbekkouri and K. E. Khatib, “Wireless Intrusion Detection Systems” in 2008.
14. M.Rehak, M. Pechoucek and P. Celeda, “Multi-Agent Approach to Network Intrusion Detection”, (Demo Paper), May, 12-16., 2008.
15. Mell, P.M, “An overview of Issues in Testing Intrusion Detection Systems”, U.S Department of Commerce, Technology Administration, National Institute of Standards & Technology, Galthersburg, July 2003.
16. N Puketza, K Zhang, M Chung, B Mukherjee, and R. A. Olsson, “A methodology for Testing intrusion detection systems”, IEEE Transactions on Software Engineering, 1996.
17. Neveen I. Ghali, “Feature Selection for Effective Anomaly-Based Intrusion Detection”. IJCSNS International Journal of Computer Science and Network Security, March 2009.
18. Peng Tao, Zuo Wanli,”Data Mining for Network Intrusion Detection System in Real Time”,IJCSNS International Journal of Computer Science and Network Security, February 2006.
19. Peter Mell and Mark McLarnon, “Mobile Agent Attack Resistant Distributed Hierarchical Intrusion Detection Systems”, 2nd International Workshop on Recent Advances in Intrusion Detection – RAID 99.
20. Phillip A. Porras and Alfonso Valdes. Live traffic analysis of tcp/ip gateways. In Proceedings of the 1998 ISOC Symposium on Network and Distributed System Security (NDSS'98), San Diego, CA, March 1998. Internet Society.
21. R. G. Bace, “Intrusion Detection”, Macmillan Technical Publishing. 2000.
22. R. Graham, “FAQ: Network Intrusion Detection Systems”. March 21, 2000.
23. Rajan Sriram Sunder, Cherukuri ijaya Krishna, “An over view of IDS”, Masters in Software Engineering, Maladalen University.
24. Robiah Yuso, Siti Rahayu Selamat, Shahrin Sahib, “Intrusion Alert Correlation Technique Analysis for Heterogeneous Log”. IJCSNS International Journal of Computer Science and Network Security,September 2008.
25. S. Kumar, “Classification and Detection of Computer Intrusions”, 1995.

26. S. Kumar, E. Spafford, “A Software architecture to Support Misuse Intrusion Detection” in The 18th National Information Security Conference, pp. 194-204. 1995.
27. S. R, Snapp , J Brentano, G. V. Dias etc,” DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and an Early Prototype”, In Proceedings of the 14th National Computer Security Conference, October 1991.
28. S.Sangeetha, V. Vaidehi, N.Srinivasan, K.V. Rajkumar,, S. Pradeep, N.Ragavan, C.Sri Sai Lokesh, I.Subadeepak, V.Prashanth, “Implementation Of Application Layer Intrusion Detection System Using Protocol Analysis”, IEEE International Conference on Signal processing, Jan 4-6, 2008.
29. Stefan Axelsson,”Understanding Intrusion Detection Through Visualisation”, PhD thesis, January, 2005.
30. V. Venkatachalam, S. Selvan, “Intrusion Detection using Improved Competitive Learning Lamstar Neural Network”, IJCSNS International Journal of Computer Science and Network Security, February 2007.
31. Yuill, Jim, S. Felix Wu Fengmin Gong, Ming- Yuh Huang “Intrusion Detection for an On-Going Attack”, 2nd International Workshop on Recent Advances in Intrusion Detection – RAID 99.